使用ISE為AnyConnect FlexVPN配置拆分排除

目錄

簡介

本文檔介紹使用ISE為與Cisco IOS® XE路由器的IKEv2 AnyConnect連線配置拆分 — 排除的過程。

必要條件

需求

思科建議您瞭解以下主題：

- 在路由器上配置AnyConnect IPsec的經驗
- 思科身份服務引擎(ISE)配置
- 思科安全使用者端(CSC)
- RADIUS通訊協定

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Catalyst 8000V(C8000V)- 17.12.04
- 思科安全使用者端 — 5.0.02075
- Cisco ISE - 3.2.0
- Windows 10

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

網路圖表

網路圖表

組態

要完成配置，請考慮以下各節。

路由器配置

1.在裝置上配置RADIUS伺服器以進行身份驗證和本地授權：

```
radius server ISE
 address ipv4 10.127.197.105 auth-port 1812 acct-port 1813
 timeout 120
 key cisco123

aaa new-model
aaa group server radius FlexVPN_auth_server
 server name ISE

aaa authentication login FlexVPN_auth group FlexVPN_auth_server
aaa authorization network a-eap-author-grp local
```

2.配置信任點以安裝路由器證書。由於路由器的本地身份驗證型別為RSA，因此裝置要求伺服器使用證書對自身進行身份驗證。有關證書建立的詳細資訊，請參閱PKI -1的證書註冊和PKI -2的證書註冊:

```
crypto pki trustpoint flex
 enrollment terminal
 ip-address none
 subject-name CN=flexserver.cisco.com
 revocation-check none
 rsakeypair flex1
 hash sha256
```

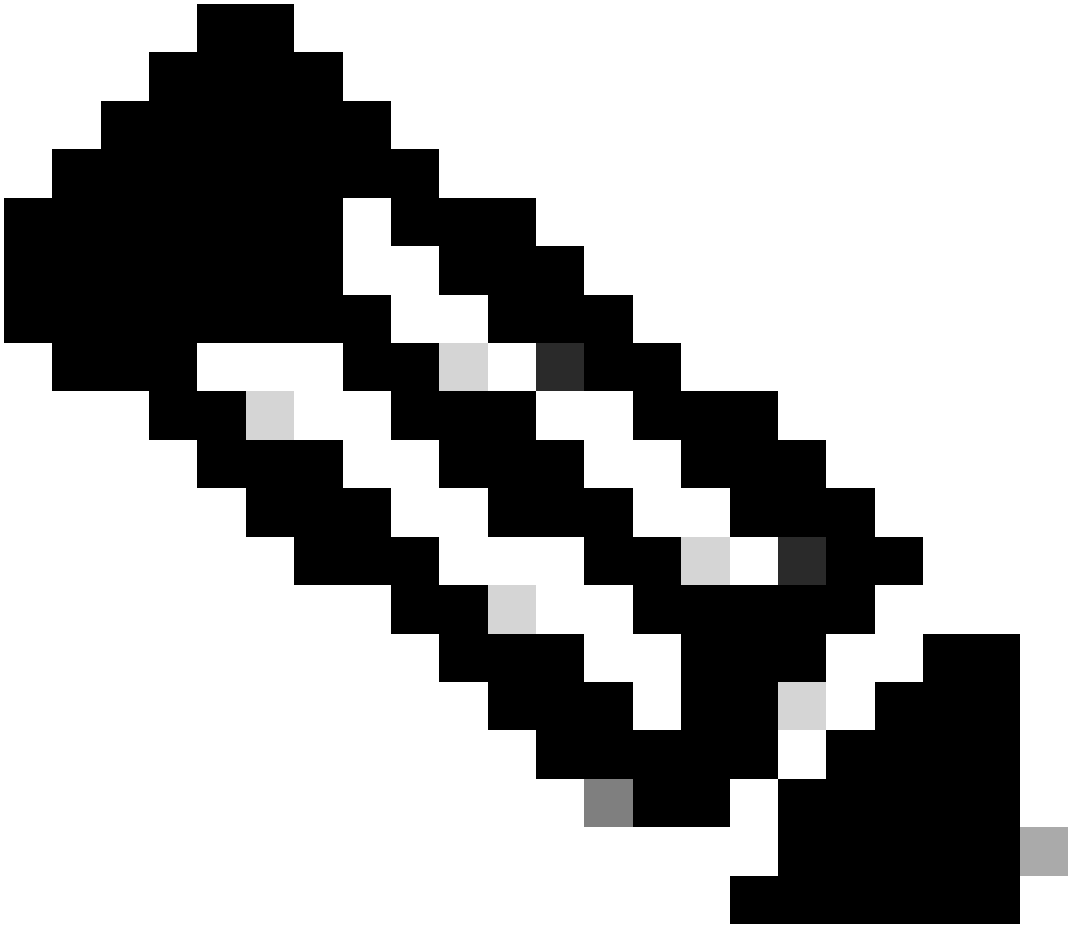
3.定義IP本地池，以便在成功AnyConnect連線時為AnyConnect VPN客戶端分配地址：

```
ip local pool ACPOOL 172.16.10.5 172.16.10.30
```

4.建立IKEv2本地授權策略：

此策略中定義的屬性以及從Radius伺服器推送的屬性將應用於使用者

```
crypto ikev2 authorization policy ikev2-auth-policy
 pool ACPOOL
 dns 8.8.8.8
```



附註：如果未配置自定義IKEv2授權策略，則使用名為default的預設授權策略進行授權。也

可以通過RADIUS伺服器推送在IKEv2授權策略中指定的屬性。您需要從RADIUS伺服器推送split-exclude屬性。

5（可選）。 建立IKEv2建議和策略（如果未配置，則使用智慧預設值）：

```
crypto ikev2 proposal IKEv2-prop1
 encryption aes-cbc-256
 integrity sha256
 group 19

crypto ikev2 policy IKEv2-pol
 proposal IKEv2-prop1
```

6（可選）。 配置轉換集（如果未配置，則使用智慧預設值）：

```
crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
mode tunnel
```

7.使用某個虛擬IP地址配置環回介面。虛擬存取介面會從其中借用IP位址：

```
interface Loopback100
 ip address 10.0.0.1 255.255.255.255
```

8.配置從中克隆虛擬訪問介面的虛擬模板：

```
interface Virtual-Template100 type tunnel
 ip unnumbered Loopback100
 ip mtu 1400
```

9.將AnyConnect客戶端配置檔案上傳到路由器的bootflash中，並按給定的定義配置檔案：

```
crypto vpn anyconnect profile acvpn bootflash:/acvpn.xml
```

10.配置包含所有連線相關資訊的IKEv2配置檔案：

```
crypto ikev2 profile prof1
 match identity remote key-id *$AnyConnectClient$*
 authentication local rsa-sig
 authentication remote eap query-identity
 pki trustpoint flex
 aaa authentication eap FlexVPN_auth
 aaa authorization group eap list a-eap-author-grp ikev2-auth-policy
 aaa authorization user eap cached
 virtual-template 100
 anyconnect profile acvpn
```

這些在IKEv2配置檔案中使用：

- match identity remote key-id *$AnyConnectClient$* — 指客戶端的標識。AnyConnect使用*$AnyConnectClient$*作為其型別為key-id的預設IKE標識。但是，可以在AnyConnect配置檔案中手動更改此標識以滿足部署需求。
- authentication remote — 提及EAP協定必須用於客戶端身份驗證。
- authentication local — 提及必須使用證書進行本地身份驗證。
- aaa authentication eap — 在EAP身份驗證期間，使用RADIUS服務器FlexVPN_auth。
- aaa authorization group eap list — 在授權過程中，網路清單a-eap-author-grp與授權策略ikev2-auth-policy一起使用。
- aaa authorization user eap cached — 啟用隱式使用者授權。
- virtual-template 100 — 定義要克隆哪個虛擬模板。
- anyconnect profile acvpn — 第9步中定義的客戶端配置檔案。在此應用於此IKEv2配置檔案。

11.配置IPsec配置檔案：

```
crypto ipsec profile AnyConnect-EAP
 set transform-set TS
 set ikev2-profile prof1
```

12.將IPsec配置檔案新增到虛擬模板：

```
interface Virtual-Template100 type tunnel
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile AnyConnect-EAP
```

13.在路由器上禁用基於HTTP-URL的證書查詢和HTTP伺服器：

```
no crypto ikev2 http-url cert
no ip http server
no ip http secure-server
```

14.配置SSL策略並將路由器的WAN IP指定為下載配置檔案的本地地址：

```
crypto ssl policy ssl-server
 pki trustpoint flex sign
 ip address local 10.106.67.33 port 443

crypto ssl profile ssl_prof
 match policy ssl-server
```

AnyConnect客戶端配置檔案（XML配置檔案）的片段：

在Cisco IOS XE 16.9.1之前的版本中，無法從頭端自動下載配置檔案。16.9.1之後，可以從頭端下載配置檔案。

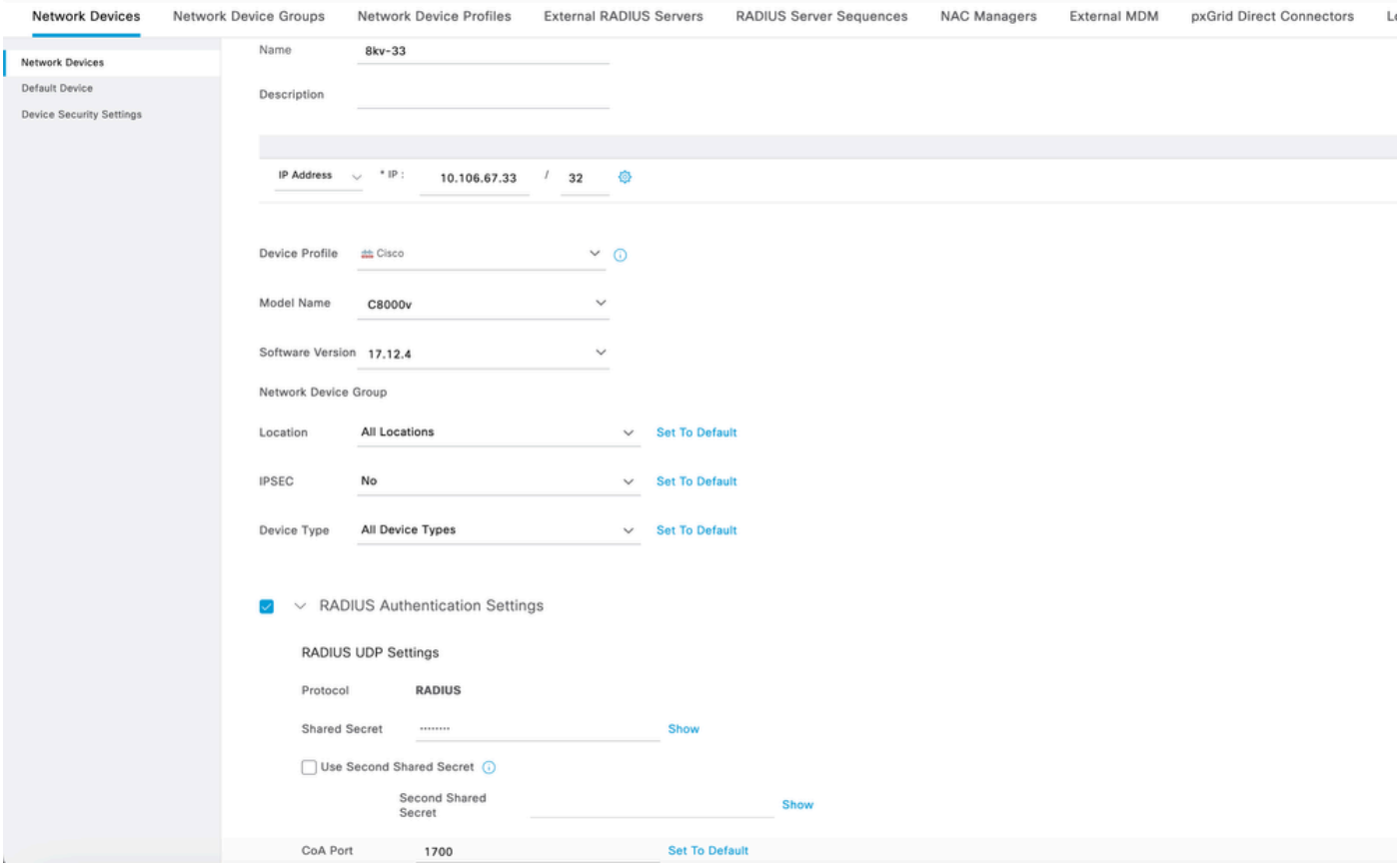
<#root>

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">false</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreMac>All</CertificateStoreMac>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<DisableCaptivePortalDetection UserControllable="true">false</DisableCaptivePortalDetection>
<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
<IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Disable
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false
</RetainVpnOnLogoff>
<AllowManualHostInput>true</AllowManualHostInput>
</ClientInitialization>
<ServerList>
```

```
<HostEntry>

<HostName>
Flex

</HostName>
<HostAddress>
flexserver.cisco.com

</HostAddress>
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>true
<AuthMethodDuringIKENegotiation>
EAP-MD5

</AuthMethodDuringIKENegotiation>
</StandardAuthenticationOnly>
</PrimaryProtocol>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

身分識別服務引擎(ISE)設定

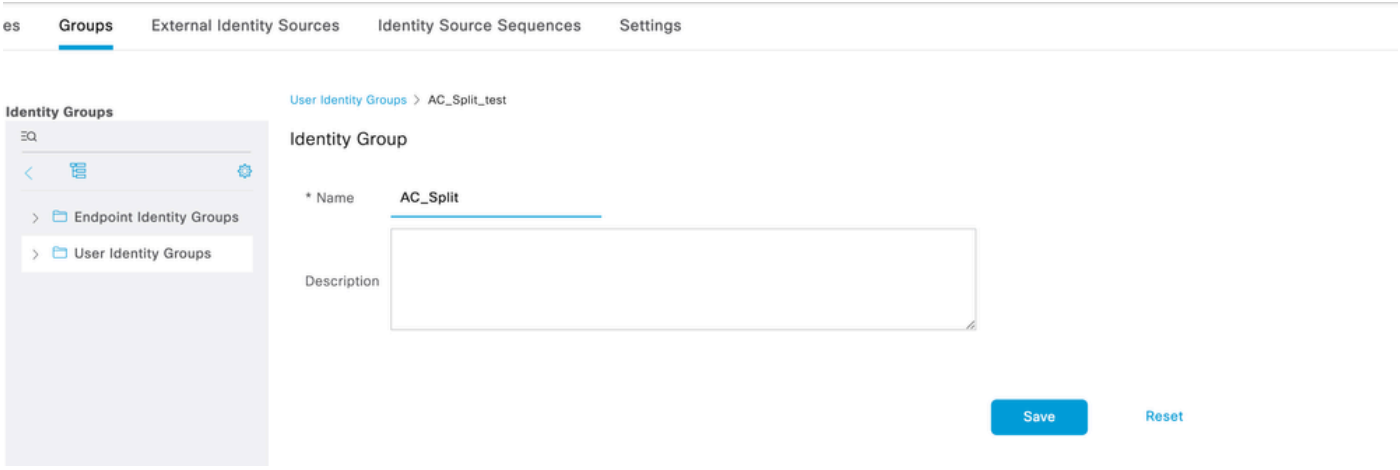
1.將路由器註冊為ISE上的有效網路裝置並為RADIUS配置共用金鑰。為此，請導航到管理>網路資源>網路裝置。按一下新增將路由器配置為AAA客戶端：



新增網路裝置

2.建立身份組：

定義身份組，以將具有相似特徵以及共用相似許可權的使用者相關聯。這些將在後續步驟中使用。導航到Administration > Identity Management > Groups > User Identity Groups，然後點選Add:



建立身份組

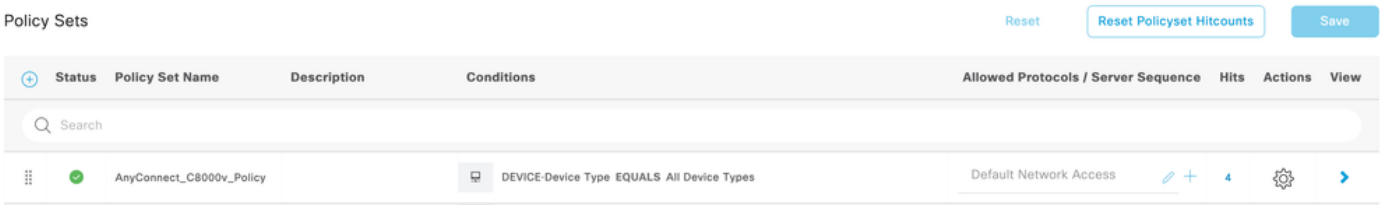
3.將使用者與身份組關聯：

將使用者關聯到正確的身份組。導航到Administration > Identity Management > Identities > Users。

將使用者新增到身份組

4. 建立策略集：

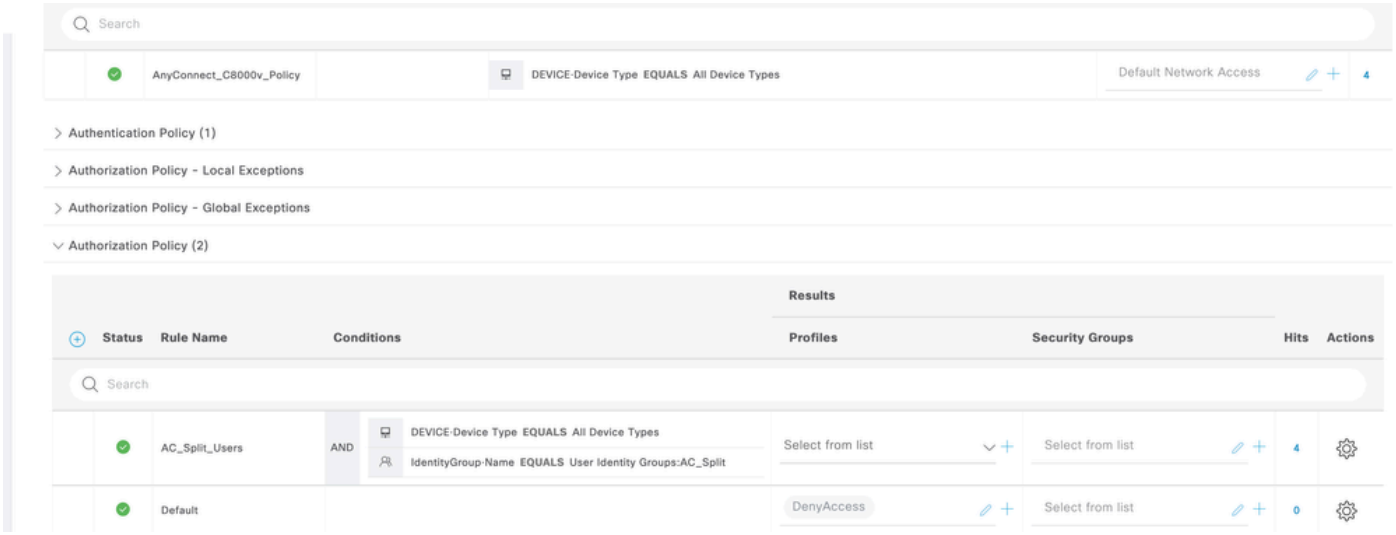
定義新的策略集並定義與策略匹配的條件。在此示例中，在這些條件下允許所有裝置型別。為此，請導航到Policy>Policy sets:



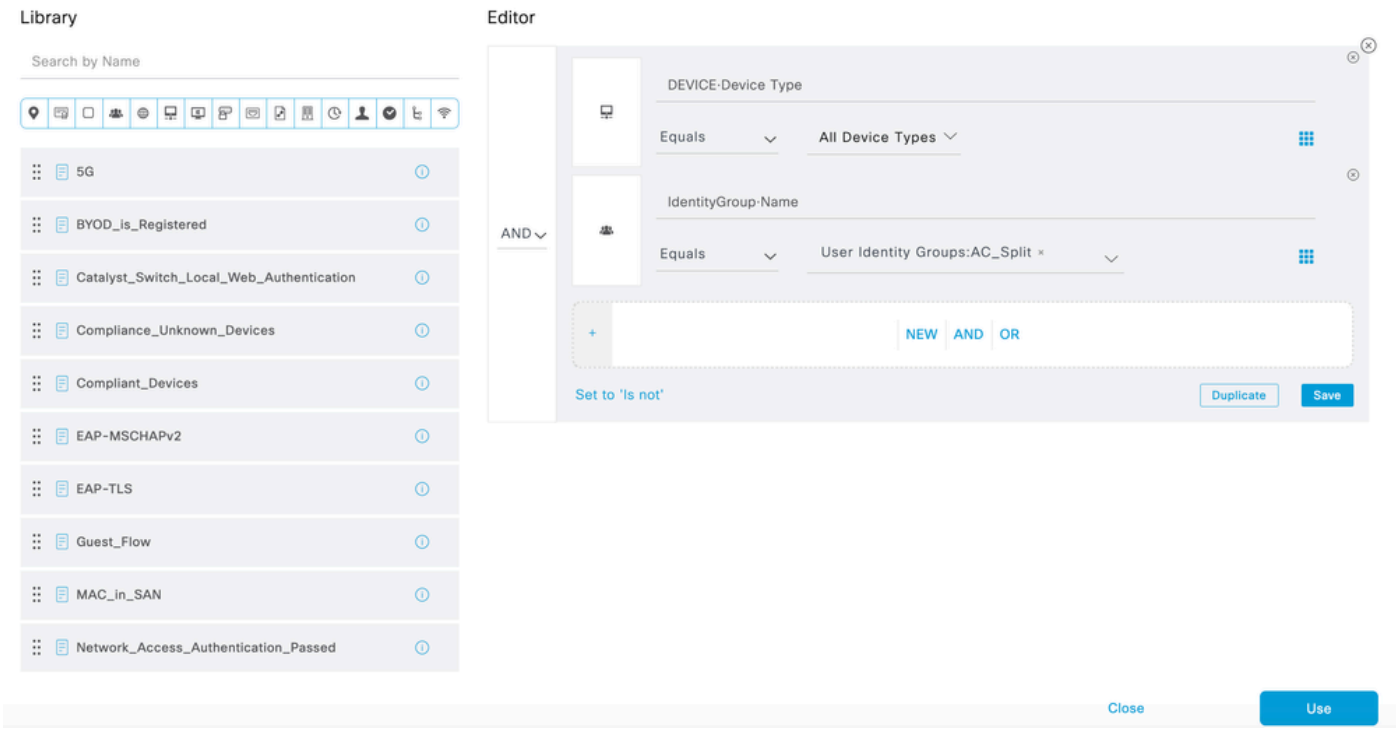
建立策略集

5.建立授權策略：

定義新的授權策略，該策略具有匹配該策略所需的條件。確保將在步驟2中建立的身份組作為條件包括在內。



建立授權策略

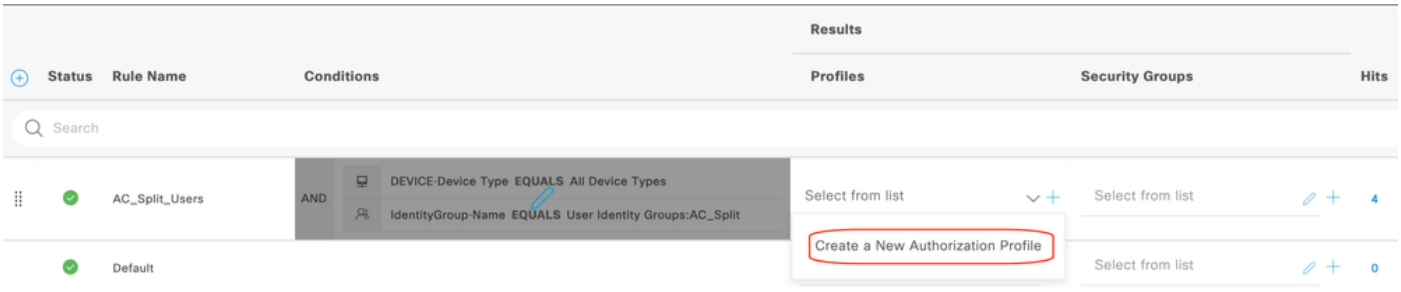


選擇授權策略中的條件

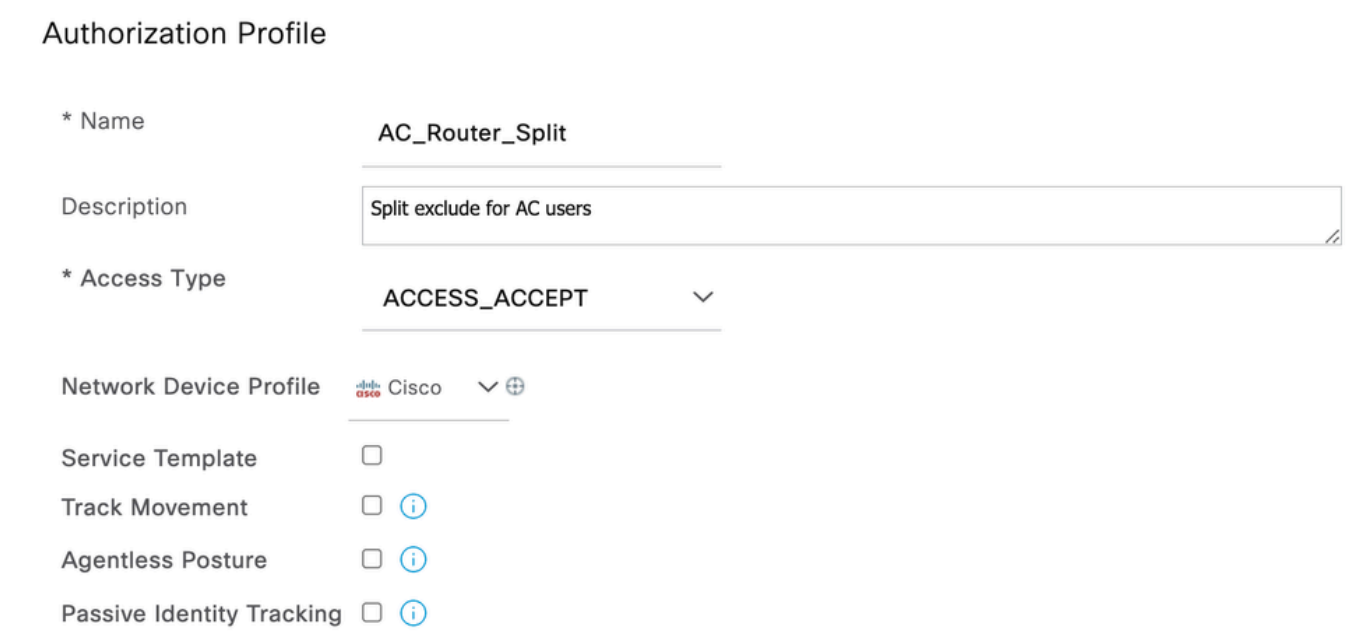
6.建立授權配置檔案：

授權配置檔案包括匹配授權策略時所執行的操作。建立新的授權配置檔案，其中包括以下屬性：

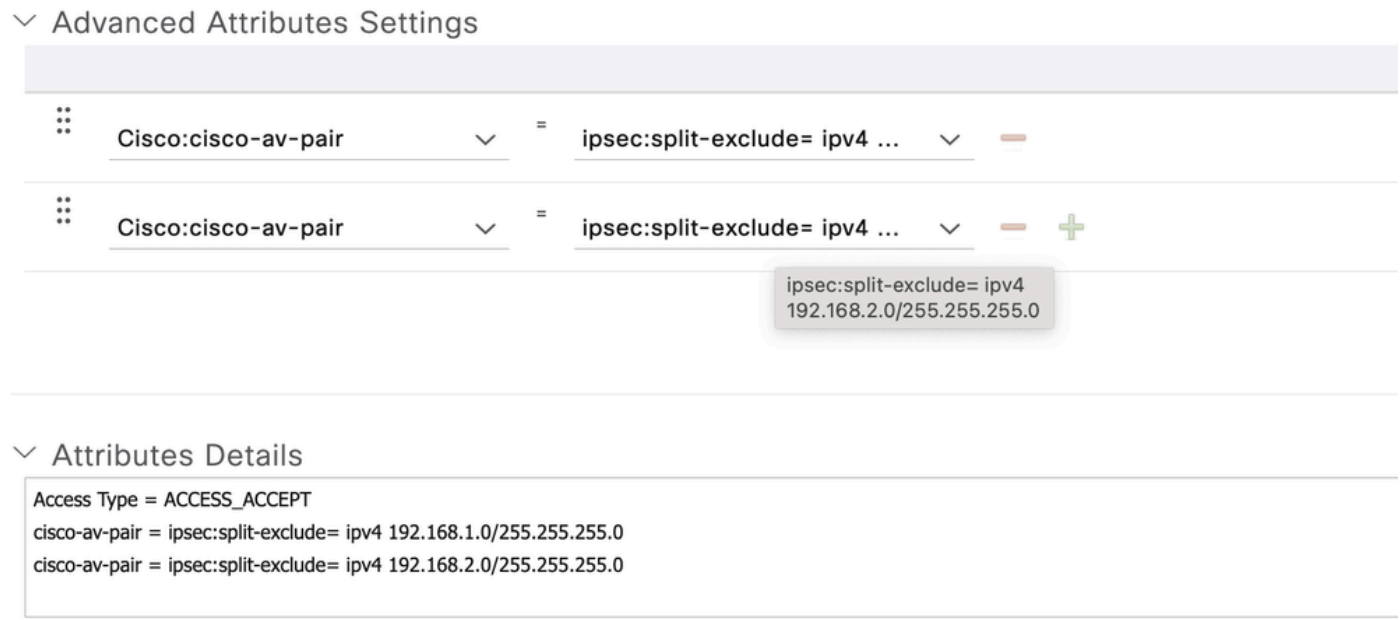
訪問型別= ACCESS_ACCEPT
cisco-av-pair = ipsec:split-exclude= ipv4 <ip_network>/<subnet_mask>



建立新的授權配置檔案

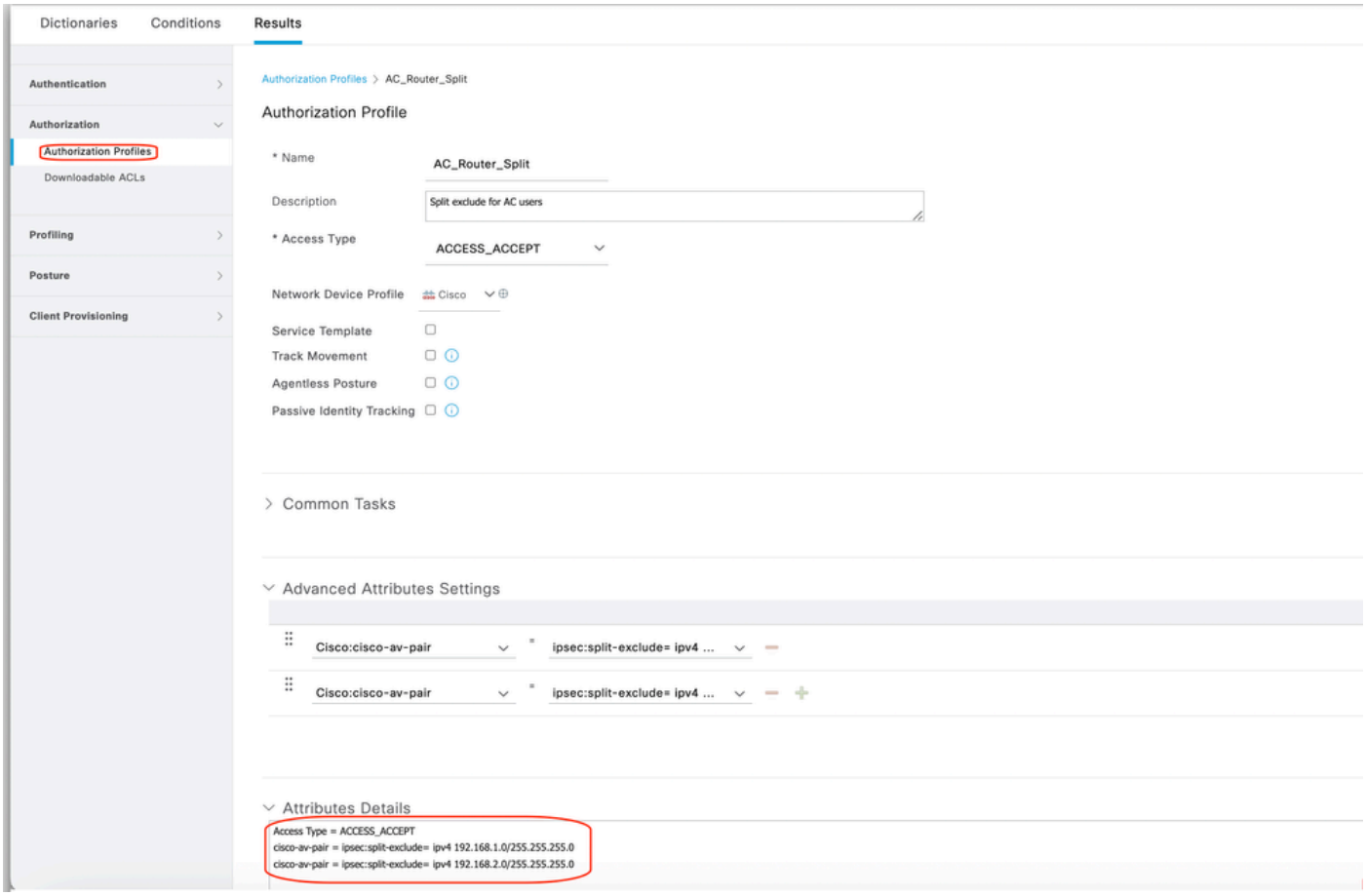


授權配置檔案配置



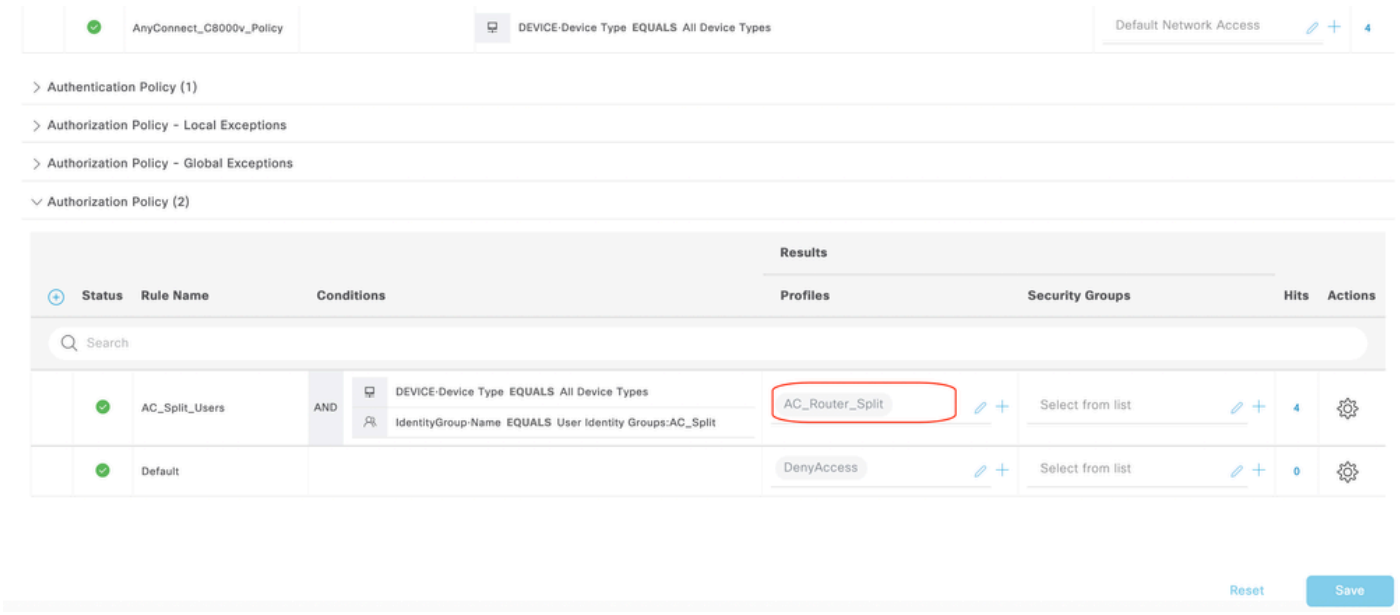
配置授權配置檔案中的屬性

7.檢查授權配置檔案配置。



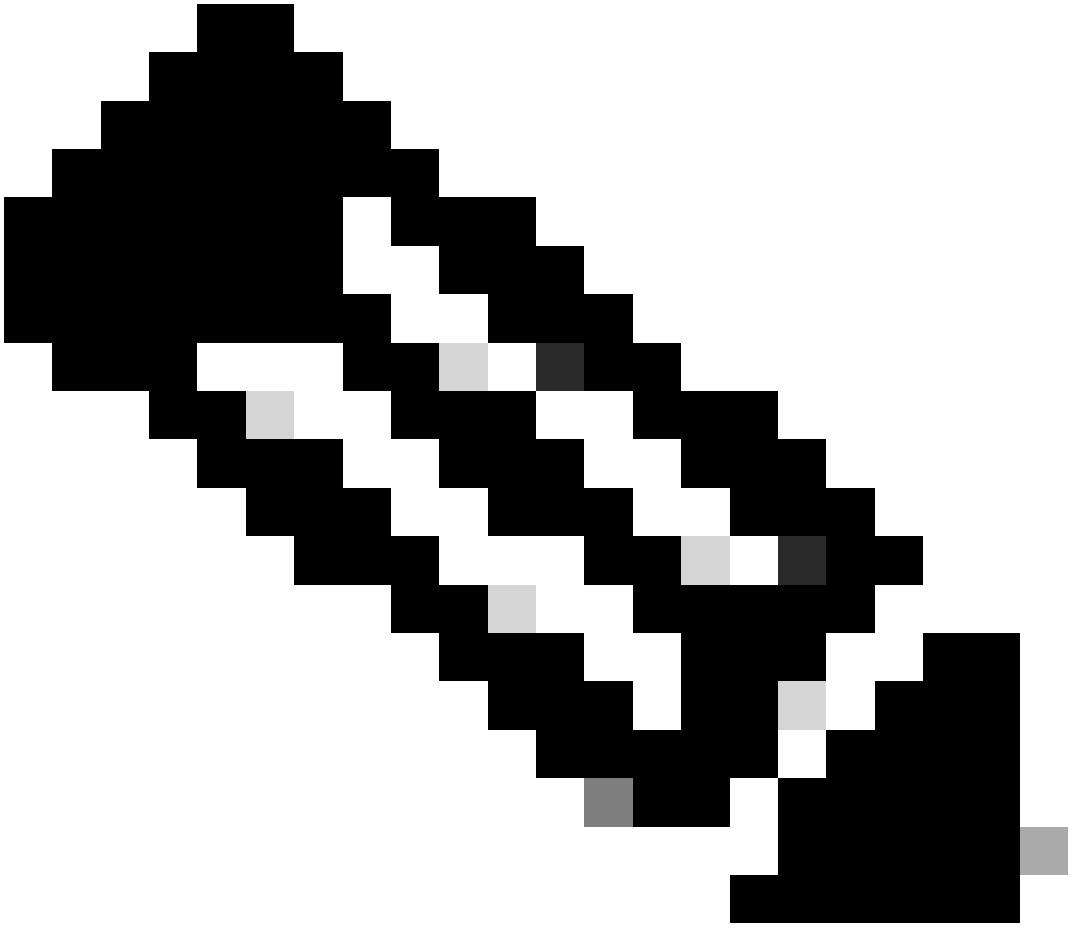
檢視授權配置檔案配置

8.這是選擇所需配置檔案後策略集配置中的授權策略：



最終授權策略配置

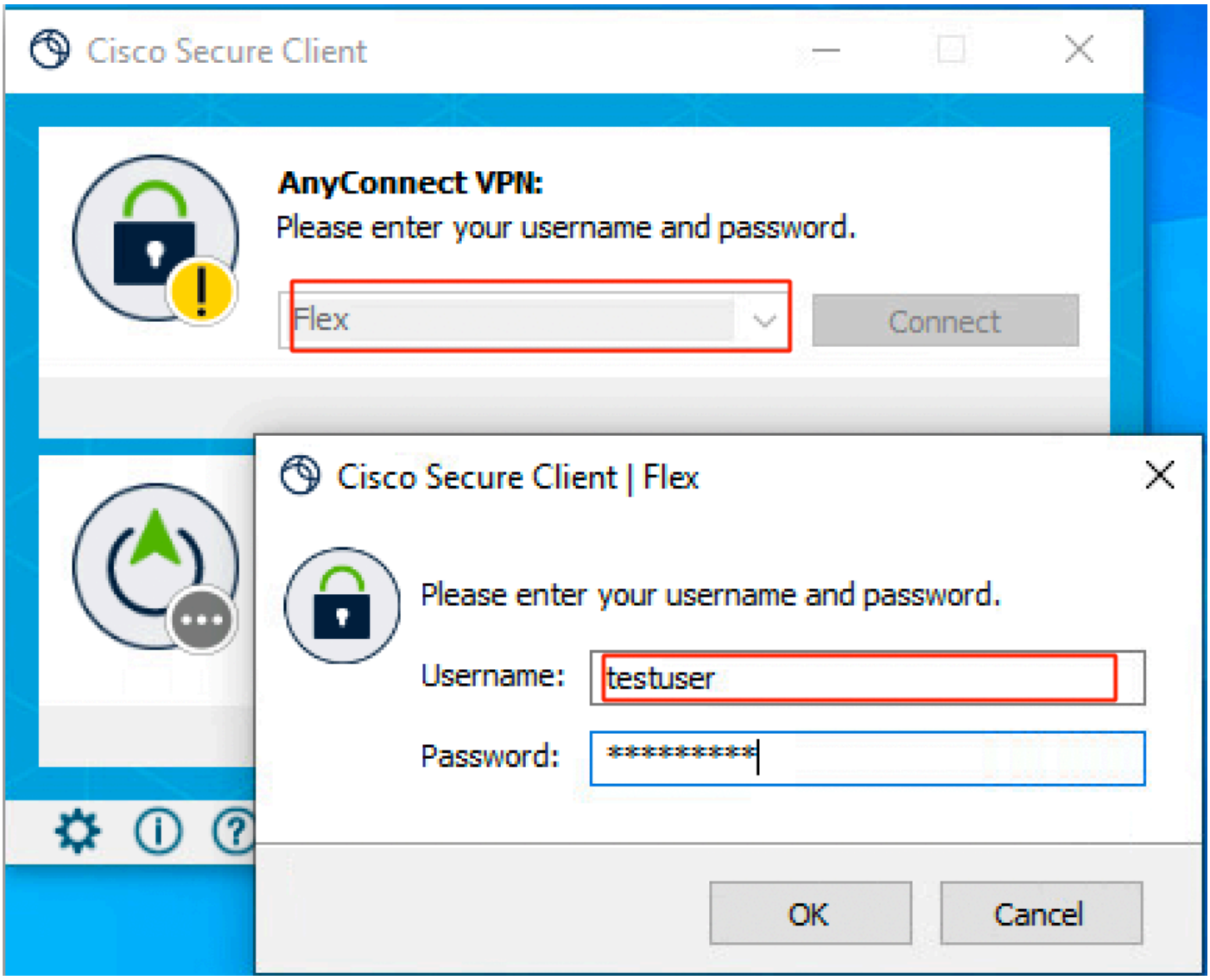
在此配置示例中，您可以根據使用者所屬的身份組排除通過VPN通過ISE配置的網路。



附註：使用Cisco IOS XE頭端進行RA VPN連線時，只能將一個拆分排除子網推送到客戶端PC。此問題已由Cisco錯誤ID CSCwj38106解決，並且多個拆分排除子網可以從17.12.4推送。有關已修復版本的更多詳細資訊，請參閱該錯誤。

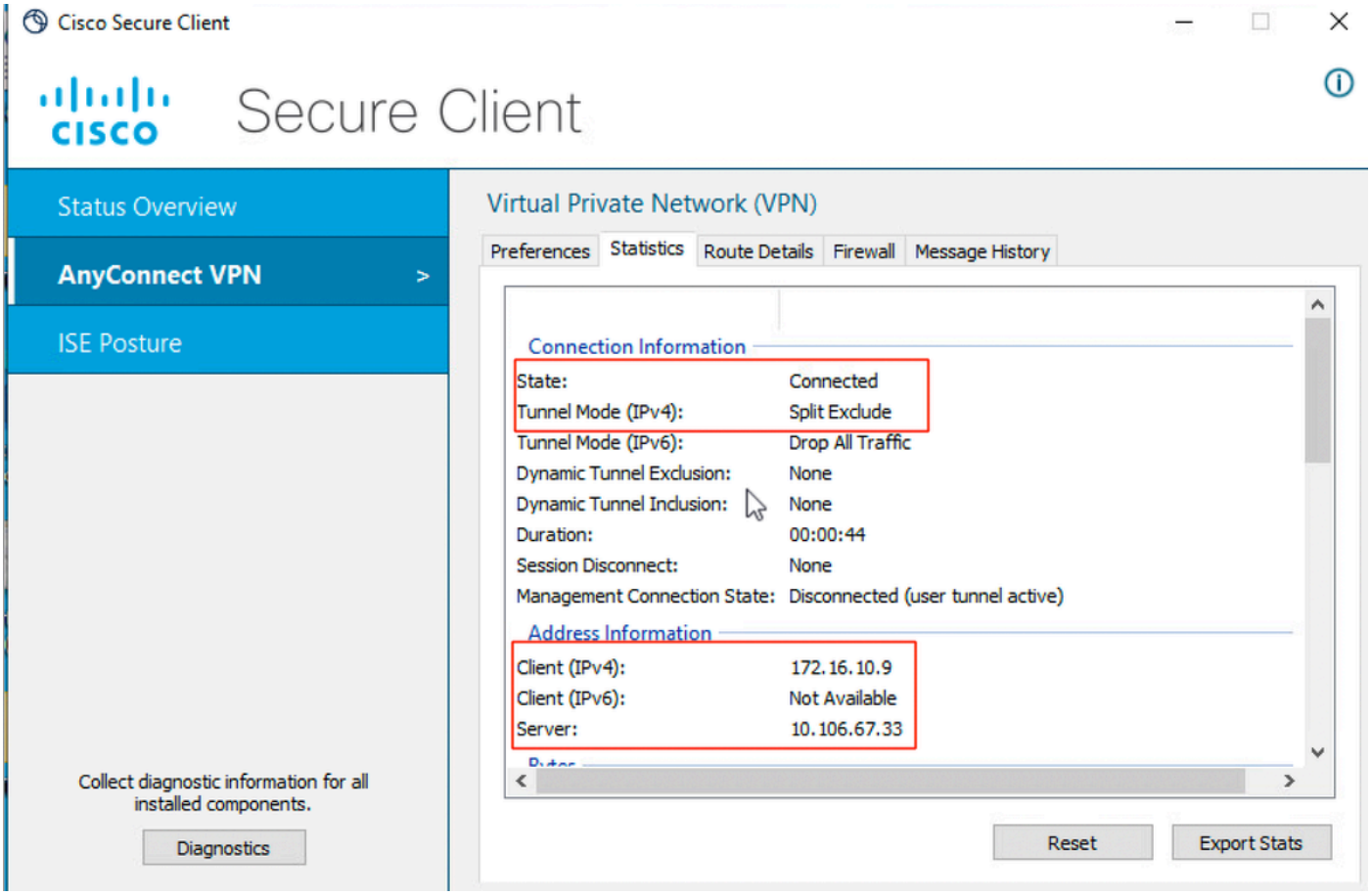
驗證

1.為了測試身份驗證，請通過AnyConnect從使用者PC連線到C8000V並輸入憑證。



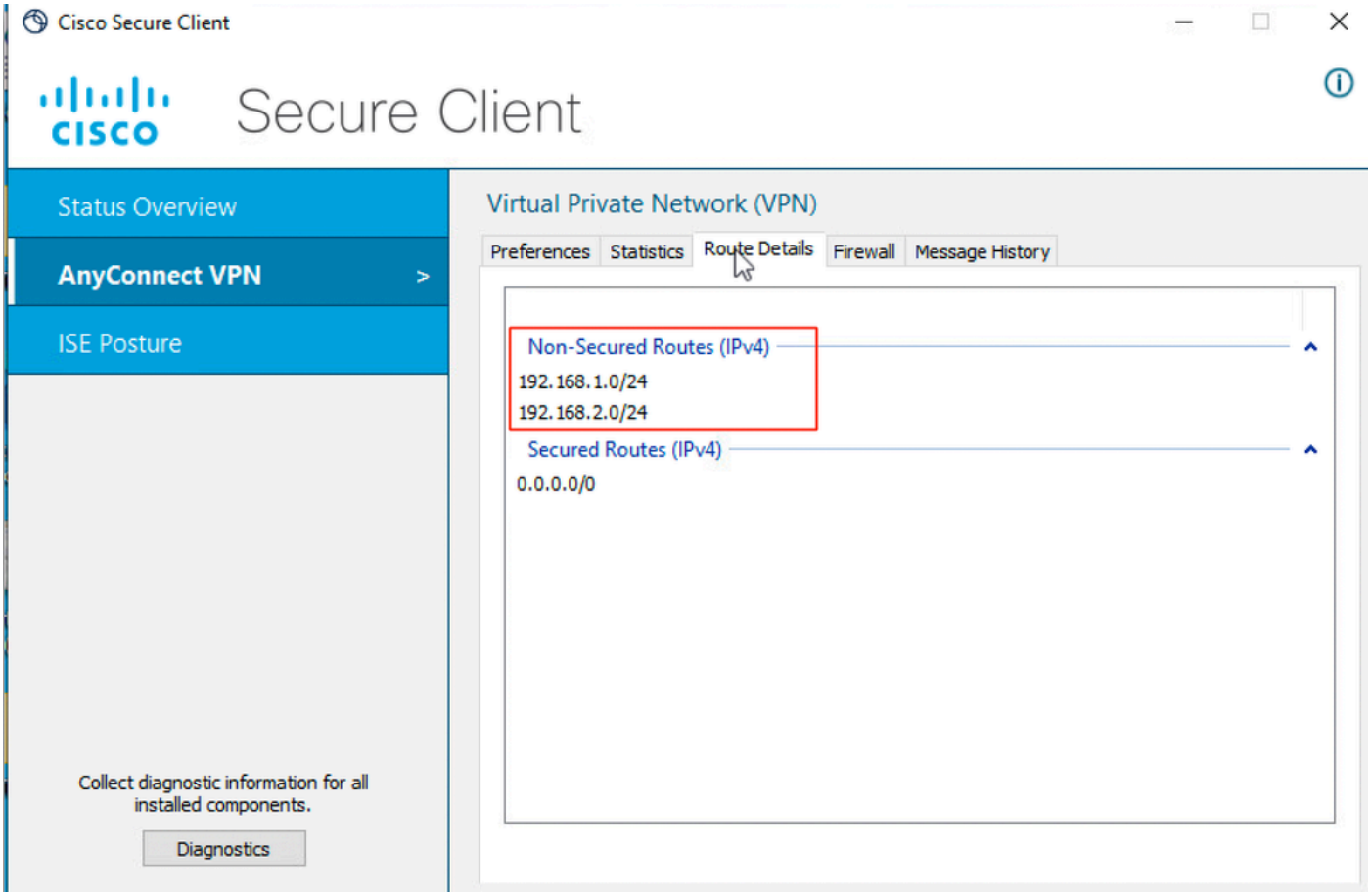
登入到AnyConnect

2.建立連線後，按一下gear圖示（左下角）並導航到AnyConnect VPN > Statistics。確認要拆分排除的隧道模式。



驗證統計資訊

導航到AnyConnect VPN > Route details，確認顯示的資訊對應於安全路由和非安全路由。



驗證路由詳細資訊

您還可以驗證VPN頭端上的連線詳細資訊：

1. IKEv2 parameters

<#root>

8kv#

show crypto ikev2 sa detail

IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status

1 10.106.67.33/4500 10.106.50.91/55811 none/none READY

Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:19, Auth sign: RSA, Auth verify: EAP

Life/Active Time: 86400/22 sec

CE id: 1012, Session-id: 6

Local spi: E8C6C5EEF0F0EF72 Remote spi: 7827644A7CA8F1A5

Status Description: Negotiation done

Local id: 10.106.67.33

Remote id: *$AnyConnectClient$*

Remote EAP id: testuser

Local req msg id: 0 Remote req msg id: 6

Local next msg id: 0 Remote next msg id: 6

Local req queued: 0 Remote req queued: 6

Local window: 5 Remote window: 1

DPD configured for 0 seconds, retry 0

Fragmentation not configured.

Dynamic Route Update: disabled

Extended Authentication configured.

NAT-T is detected outside

Cisco Trust Security SGT is disabled

Assigned host addr: 172.16.10.10

Initiator of SA : No

Post NATed Address : 10.106.67.33

PEER TYPE: Other

IPv6 Crypto IKEv2 SA

2.This is the crypto session detail for the VPN session:

<#root>

8kv#

show crypto session detail

Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal, T - cTCP encapsulation

X - IKE Extended Authentication, F - IKE Fragmentation

R - IKE Auto Reconnect, U - IKE Dynamic Route Update

S - SIP VPN

Interface: Virtual-Access1

Profile: prof1

Uptime: 00:00:44

Session status: UP-ACTIVE

Peer: 10.106.50.91 port 55811 fvrf: (none) ivrf: (none)

Phase1_id: *$AnyConnectClient$*

Desc: (none)

Session ID: 16

IKEv2 SA: local 10.106.67.33/4500 remote 10.106.50.91/55811 Active

Capabilities:NX connid:1 lifetime:23:59:16

IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 172.16.10.10

Active SAs: 2, origin: crypto map

Inbound: #pkts dec'ed 114 drop 0 life (KB/Sec) 4607987/3556

```
Outbound: #pkts enc'ed 96 drop 0 life (KB/Sec) 4608000/3556
```

3. Verify on ISE live logs.

疑難排解

在Cisco Router上:

1. 使用IKEv2和IPsec調試驗證頭端和客戶端之間的協商。

```
debug crypto condition peer ipv4 <public_ip>
debug crypto ikev2
debug crypto ikev2 packet
debug crypto ikev2 error
debug crypto ikev2 internal
debug crypto ipsec
debug crypto ipsec error
```

2. 使用AAA調試驗證本地和/或遠端屬性的分配。

```
debug aaa authorization
debug aaa authentication
debug radius authentication
```

在ISE上：

導航到操作>即時日誌使用RADIUS即時日誌。

工作場景

這是成功連線的調試：

<#root>

```
*Oct 13 10:01:25.928: RADIUS/ENCODE(0000012D):Orig. component type = VPN IPSEC
*Oct 13 10:01:25.929: RADIUS/ENCODE(0000012D): dropping service type, "radius-server attribute 6 on-for
*Oct 13 10:01:25.929: RADIUS(0000012D): Config NAS IP: 0.0.0.0
*Oct 13 10:01:25.929: vrfid: [65535] ipv6 tableid : [0]
*Oct 13 10:01:25.929: idb is NULL
*Oct 13 10:01:25.929: RADIUS(0000012D): Config NAS IPv6: ::
*Oct 13 10:01:25.929: RADIUS/ENCODE(0000012D): acct_session_id: 4291
*Oct 13 10:01:25.929: RADIUS(0000012D): sending
*Oct 13 10:01:25.929: RADIUS/ENCODE: Best Local IP-Address 10.106.67.33 for Radius-Server 10.127.197.10
*Oct 13 10:01:25.929: RADIUS: Message Authenticator encoded
*Oct 13 10:01:25.929: RADIUS(0000012D): Send Access-Request to 10.127.197.105:1812 id 1645/24, len 344
```

```
RADIUS: authenticator 85 AC BF 77 BF 42 0B C7 - DE 85 A3 9A AF 40 E5 DC
*Oct 13 10:01:25.929: RADIUS: Service-Type [6] 6 Login [1]
*Oct 13 10:01:25.929: RADIUS: Vendor, Cisco [26] 26
*Oct 13 10:01:25.929: RADIUS: Cisco AVpair [1] 20 "service-type=Login"
*Oct 13 10:01:25.929: RADIUS: Vendor, Cisco [26] 45
```

***Oct 13 10:01:25.929: RADIUS: Cisco AVpair [1] 39 "isakmp-phase1-id=*$AnyConnectClient$*"**

```
*Oct 13 10:01:25.929: RADIUS: Calling-Station-Id [31] 14 "10.106.50.91"
*Oct 13 10:01:25.929: RADIUS: Vendor, Cisco [26] 64
*Oct 13 10:01:25.929: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L40A6A4321ZO2L40A6A325BZH1194CC58
*Oct 13 10:01:25.929: RADIUS: User-Name [1] 10 "testuser"
*Oct 13 10:01:25.929: RADIUS: Vendor, Cisco [26] 21
*Oct 13 10:01:25.929: RADIUS: Cisco AVpair [1] 15 "coa-push=true"
*Oct 13 10:01:25.929: RADIUS: EAP-Message [79] 24
RADIUS: 02 8E 00 16 04 10 8A 09 BB 0D 4B A9 D6 2B 59 1C C8 FE 1C 90 56 F5 [ K+YV]
*Oct 13 10:01:25.929: RADIUS: Message-Authenticato[80] 18
RADIUS: 54 85 1B AC BE A8 DA EF 24 AE 4D 28 46 32 8C 48 [ T$M(F2H]
*Oct 13 10:01:25.929: RADIUS: State [24] 90
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 30 41 36 41 34 33 32 31 5A 4F 32 4C 34 [2L40A6A4321ZO2L4]
RADIUS: 30 41 36 41 33 32 35 42 5A 48 31 31 39 34 43 43 [0A6A325BZH1194CC]
RADIUS: 35 38 5A 4E 31 32 3B 33 30 53 65 73 73 69 6F 6E [58ZN12;30Session]
RADIUS: 49 44 3D 69 73 65 2D 70 73 6E 2F 35 31 37 31 33 [ID=ise-psn/51713]
RADIUS: 35 39 30 30 2F 33 38 3B [ 5900/38;]
*Oct 13 10:01:25.929: RADIUS: NAS-IP-Address [4] 6 10.106.67.33
*Oct 13 10:01:25.929: RADIUS(0000012D): Sending a IPv4 Radius Packet
*Oct 13 10:01:25.929: RADIUS(0000012D): Started 120 sec timeout
```

***Oct 13 10:01:25.998: RADIUS: Received from id 1645/24 10.127.197.105:1812, Access-Accept, len 239**

```
RADIUS: authenticator BC 19 F2 EE 10 67 80 C5 - 9F D9 30 9A EA 7E 5E D3
*Oct 13 10:01:25.998: RADIUS: User-Name [1] 10 "testuser"
*Oct 13 10:01:25.998: RADIUS: Class [25] 67
RADIUS: 43 41 43 53 3A 4C 32 4C 34 30 41 36 41 34 33 32 [CACS:L2L40A6A432]
RADIUS: 31 5A 4F 32 4C 34 30 41 36 41 33 32 35 42 5A 48 [1ZO2L40A6A325BZH]
RADIUS: 31 31 39 34 43 43 35 38 5A 4E 31 32 3A 69 73 65 [1194CC58ZN12:ise]
RADIUS: 2D 70 73 6E 2F 35 31 37 31 33 35 39 30 30 2F 33 [-psn/517135900/3]
RADIUS: 38 [ 8]
*Oct 13 10:01:25.998: RADIUS: EAP-Message [79] 6
RADIUS: 03 8E 00 04
*Oct 13 10:01:25.998: RADIUS: Message-Authenticato[80] 18
RADIUS: F9 61 C1 FD 6D 26 31 A2 89 04 72 BC DD 32 A9 29 [ am&1r2)]
*Oct 13 10:01:25.998: RADIUS: Vendor, Cisco [26] 59
```

***Oct 13 10:01:25.998: RADIUS: Cisco AVpair [1] 53 "ipsec:split-exclude= ipv4 192.168.1.0/255.255.255.0"**

```
*Oct 13 10:01:25.998: RADIUS: Vendor, Cisco [26] 59
```

***Oct 13 10:01:25.998: RADIUS: Cisco AVpair [1] 53 "ipsec:split-exclude= ipv4 192.168.2.0/255.255.255.0"**

```
*Oct 13 10:01:25.998: RADIUS(0000012D): Received from id 1645/24
RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
8kv#
```

參考資料

- 使用本地使用者資料庫為IKEv2遠端訪問配置FlexVPN頭端
- 配置採用EAP和DUO身份驗證的AnyConnect Flexvpn
- 使用EAP-MD5配置AnyConnect IKEv2遠端訪問

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。